IN THE CLAIMS

1.- 6. (Canceled)

7. (currently amended) A method wherein a trusted party authenticates, for the benefit of a third party, that a customer using an account during an online transaction with said third party is the actual owner of said account, said third party desiring verification as to the identity of said customer before proceeding with said online transaction with said customer, said method comprising:

requesting over a network, by said trusted party from said customer during said online transaction, of an identity-authenticating password;

verifying, by said trusted party, that said identity-authenticating password from said customer matches a password previously designated for said account; and

notifying said ~~a~~ third party over said network during said online transaction, by said trusted party, that said customer is the actual owner of said account when said identity-authenticating password entered by said customer matches the password that was previously designated for said account, whereby said trusted party authenticates said customer for said third party during said online transaction ~~said notified third party desires verification as to the identity of said customer before proceeding with an online transaction with said customer~~.

8. (currently amended) A method as recited in claim 7 wherein said trusted party is an issuer financial institution and said third party is an online merchant, whereby said online merchant conducts an online ~~a~~ financial transaction with said customer, and wherein said account of said customer is maintained by said issuer financial institution.

9. (previously presented) A method as recited in claim 7 further comprising:

querying an access control server to determine if an account of said customer is enrolled in a payment authentication service.

10. (previously presented) A method as recited in claim 9 wherein the access control server determines if said customer account is enrolled by verifying that said customer account is contained in a database of enrolled customer accounts.

11. (previously presented) A method as recited in claim 9 further comprising:

querying a directory server to verify that said customer account is associated with an issuer financial institution that is participating in said payment authentication service, whereby said customer account is not enrolled with said payment authentication service if said customer account is not associated with an issuer financial institution.

12. (previously presented) A method as recited in claim 11 further comprising:

sending to said third party's computer system an Internet address for said access control server, said Internet address passing through said directory server before reaching said third party's computer system, whereby said Internet address for said access control server allows said third party to directly communicate with said access control server.

13. (previously presented) A method as recited in claim 9 further comprising:

reviewing a memory device controlled by said third party to verify that said customer account is associated with an issuer financial institution participating in said payment authentication service, whereby said customer account is not enrolled with said payment authentication service if said customer account is not associated with an issuer financial institution.

14. (currently amended) A method as recited in claim 7 further comprising:

generating, by said trusted party, a digitally-signed transaction receipt using a signature key of said trusted party; and

sending, by said trusted party, said ~~of a~~ digitally-signed transaction receipt to said third party, whereby said ~~the~~ digitally-signed transaction receipt confirms to said third party that the identity of said customer has been authenticated.

15. (previously presented) A method as recited in claim 14 wherein said transaction receipt includes a number associated with said customer account, a transaction payment amount, and a transaction payment date.

16. (previously presented) A method as recited in claim 7 further comprising:

sending, by said trusted party, of a card authentication verification value to said third party, the card authentication verification value containing a unique value for said customer account and a specific payment transaction, whereby said card authentication verification value

uniquely identifies a specific authenticated payment transaction.

17. (currently amended) A method as recited in claim 14 ~~8~~ further comprising:

verifying, by said third party, ~~of~~ said digitally signed transaction receipt such that said third party is assured that said transaction receipt was sent from a specific trusted party.

18. (previously presented) A method as recited in claim 7 further comprising:

sending, by said third party, of an authorization message to an issuer financial institution to verify said customer account has adequate credit for a requested purchase.

19. (previously presented) A method as recited in claim 7 wherein said customer enrolls in said payment authentication service, the method further comprising:

receiving, by said trusted party, of enrollment information entered at an enrollment Internet web site by said customer;

verifying, by said trusted party, that said enrollment information substantially matches information contained within a pre-existing database of customer information; and

storing said customer account information in a database for enrolled customer accounts.

20. (currently amended) A method performed by a payment authentication service wherein a trusted party authenticates, for the benefit of a third party, that a customer using an account during an online transaction with said third party is the actual owner of said account, said method comprising:

sending an authentication ~~a payment~~ request message via ~~to~~ a customer computer ~~software module~~ from a third-party software module over a network during said online transaction;

receiving said authentication ~~a payment~~ request message at an access control server that is operated by said trusted party~~, said payment request message being sent to said access control server from said customer software module~~;

requesting over said network, by said trusted party, of a password from said customer;

verifying, by said trusted party, that said password entered by said customer is valid; and

sending over said network, by said trusted party, an authentication ~~a payment~~ response message to a third-party software module, said payment response message containing an authentication status indicator, whereby said trusted party authenticates said customer for said third party.

21. (currently amended) A customer software module of a customer computer containing computer code used with a payment authentication service wherein an issuer financial institution authenticates, for the benefit of a third party, that a customer using an account during an online transaction with said third party is the actual owner of said account, said customer software module effecting the following:

receiving an authentication ~~a payment~~ request message from said ~~a~~ third party during said online transaction that requests the initiation of a payment authentication service wherein the identity of said ~~a~~ customer will be authenticated;

sending said authentication ~~payment~~ request message to an access control server operated by said issuer financial institution, said customer having an account with said issuer financial institution; ~~and~~

receiving a request from said access control server for said customer to enter a password used to verify the identity of said customer; and

facilitating the sending of an authentication response message from said access control server to said third party via said customer computer regarding the verification of the identity of said customer, whereby said access control server verifies the identity of said customer for said third party.

22. - 31. (Canceled)

Please add the following new claims:

32. (New) A method performed by a payment authentication service wherein a trusted party authenticates a customer for the benefit of a third party, said method comprising:

receiving a request over a network from a customer computer to perform a financial transaction with said third party;

determining that said customer is enrolled in said payment authentication service;

sending an authentication request message from said third party via said customer computer over a network during said financial transaction, said authentication request message destined for a computer of said trusted party;

receiving an authentication response message from said computer of said trusted party via said customer computer during said financial transaction, said authentication response message indicating the authenticity of said customer, said authenticity being based upon a password supplied by said customer to said computer of said trusted party, whereby said trusted party authenticates said customer for said third party.

33. (New) A method as recited in claim 7 wherein said online transaction is a payment transaction.

34. (New) A method as recited in claim 20 wherein said online transaction is a payment transaction.

35. (New) A method as recited in claim 21 wherein said online transaction is a payment transaction.

36. (New) A method as recited in claim 32 wherein said financial transaction is a payment transaction.

37. (New) A method as recited in claim 20 wherein said payment authentication service uses a centralized architecture, and wherein said third-party software module sends said authentication request message to said access control server by way of a browser in said customer computer.

38. (New) A method as recited in claim 20 wherein said payment authentication service uses a distributed architecture, wherein said third-party software module sends said authentication request message to a software module of said customer computer and wherein said customer computer then sends said authentication request message to said access control server.

39. (New) A method as recited in claim 32 wherein said payment authentication service uses a centralized architecture, and wherein said third party sends said authentication request message to said trusted party computer by way of a browser in said customer computer.

40. (New) A method as recited in claim 32 wherein said payment authentication service uses a distributed architecture, wherein said third party sends said authentication request message to a software module of said customer computer and wherein said customer computer then sends said authentication request message to said trusted party computer.